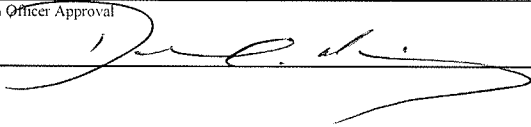




King County Information Technology Governance Policies & Standards

Policy Title Enterprise Information Security Policy	Document Code No.
Chief Information Officer Approval 	Effective Date February 28, 2005

1.0 PURPOSE:

This policy establishes the principles for the county's security practices and the foundation for developing and complying with countywide information security policies and standards through a long term and ongoing process implemented at various stages.

Information security is both a technical and a business issue and is every county information technology user's responsibility. Effective information security requires the active engagement of county management to assess emerging security threats to their business and provide strong information security leadership.

2.0 APPLICABILITY:

Applicable to King County Government.

3.0 REFERENCES:

- 3.1 ISO 17799
- 3.2 NIST CSRC Special Publications
- 3.3 National Security Association (NSA) Security Configuration Guides

4.0 DEFINITIONS:

- 3.4 **Asset:** Component of a business process and can include computer rooms, networks, digital and paper records, hardware, software, people, and data.
- 3.5 **Availability:** The assurance that a computer system is accessible by authorized users whenever needed or as pre-defined.
- 3.6 **Confidentiality:** An attribute of information. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial.
- 3.7 **Information processing facility:** A facility, separate from general office space, that contains a data center, network operations center, or other similar information system command or monitoring center with computer systems that store production information or house network services.
- 3.8 **Information system:** Software, hardware and interface components that work together to perform a set of business functions.
- 3.9 **Information system lifecycle:** The course of developmental changes through which a system passes from its conception to the termination of its use and subsequent salvage,

including phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of the system.

- 3.10 **Integrity:** The condition of data or a system, which is that it remains intact, unaltered, and hence reliable.
- 3.11 **ISO:** Acronym for the International Organization for Standards. In Greek, ISO means “equal”. It is the universal acronym used to identify this international standards setting body. ISO/IEC 17799 is the international standard for Information Technology – Code of practice for information security technology. This standard is also known as BS 7799.
- 3.12 **NIST CSRC:** Acronym for the National Institute of Standards and Technology, Computer Security Resource Center. NIST produces security guidelines for use by Federal government organizations.
- 3.13 **Organization:** Every county office, every officer, every institution, whether educational, correctional or other, and every department, division, board and commission.
- 3.14 **Risk:** Threats to, impacts on, and vulnerabilities of information and information processing facilities.
- 3.15 **Security:** An attribute of information systems which includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services and the privacy of individuals.
- 3.16 **Security control:** Technical or non-technical process employed by an organization to protect information systems, detect breaches in its information security, and mitigate information security risks.
- 3.17 **Security guideline:** Recommended actions and/or industry best practices that should be used to guide security practices by users, IT staff and others. Security guidelines are not compulsory.
- 3.18 **Security practice:** Typical and customary way of managing security that is either formalized through security policies, standards and procedures, or is informal, reactive, and ad hoc in nature.
- 3.19 **Security policy:** Set of organizational rules and practices (specified or implied) that regulate how an organization manages, protects and uses its information system assets and data. These are rigid and must be complied with. Any exceptions to these must be documented, reviewed and approved. Security policies are a blueprint for an organization’s security program.
- 3.20 **Security standard:** Rules indicating how and what kind of software, hardware, databases, and business processes must be implemented, used and maintained to meet security and operational objectives. Security standards are compulsory.

- 3.21 **Third party:** Any person, group of persons or organization who has a business relationship with the county.

5.0 POLICIES:

- 5.1 **Security Principles** - King County information is a valuable asset. Information shall be protected from unauthorized disclosure, modification, or destruction, and shall be safeguarded to the extent required by law. King County information security practices shall conform to the following principles:
- 5.1.1 **Accountability** - Information security accountability and responsibility should be clearly defined as part of a security management structure and be acknowledged by staff and management.
 - 5.1.2 **Assessment** - Risks to information and information systems should be assessed periodically and be continually managed as part of a information security risk management program to address vulnerabilities and threats.
 - 5.1.3 **Awareness** - Anyone with access to King County's information systems and networks, should be aware of the need for information security and be trained in what they can do to enhance security to support the county's business.
 - 5.1.4 **Cost Effective** - Information security controls should be cost-effective and proportionate to the risks.
 - 5.1.5 **Equity** - Organizations should respect the rights of one another and their actions in King County's shared information environment should be ethical and not adversely affect others.
 - 5.1.6 **Integration** - Information security is an important element of sound business management and should be an integral part of the county's information system lifecycle.
 - 5.1.7 **Management** - Information security policies, standards, procedures and practices should be developed and implemented based on industry recognized security standards, periodically tested and evaluated, and corrective actions taken to remediate identified deficiencies.
 - 5.1.8 **Timeliness** - Organizations should act in a timely, coordinated manner to prevent, detect and respond to breaches of and threats to information security.
- 5.2 **Countywide policies** - Specific countywide information security policies, standards, guidelines and practices shall be implemented to ensure that integrity, confidentiality, and availability of county information are not compromised.
- 5.2.1 **Policy foundation** - These countywide policies, standards and guidelines shall be based on industry recognized security standards, such as ISO 17799, NIST CSRC Special Publications, and National Security Association (NSA) Security Configuration Guides.

- 5.2.2 **Minimum requirement** - These countywide policies and standards shall be considered minimum requirements to provide a secure environment for developing, implementing, and supporting information technology and systems.

5.3 Countywide security

- 5.3.1 **Technology Management Board (TMB) Security Sub Team** - The TMB security sub team shall focus on countywide information security and membership shall consist of organization representatives.

5.4 Organization security

- 5.4.1 **Organization policies** - Organizations may develop more stringent policies and standards as needed to handle organization-specific cases.
- 5.4.2 **Organization procedures** - Organizations shall develop and document procedures that support the countywide information security policies, standards and guidelines.

5.5 Compliance

- 5.5.1 **Annual compliance review** - At least annually, organizations shall review their information security processes, procedures and practices and any agency specific policies and standards, for compliance with this policy.
- 5.5.2 **Verification of compliance** - Annually the executive, judiciary, council and all other elected officials shall verify in writing to the chief information officer that the organization is in compliance with this policy and identify any areas where compliance has not been achieved
- 5.5.3 **Annual review** - Annually the CIO shall review the status of organization adoption and compliance with countywide information security policies and standards and works with organizations on any required compliance follow-up.

6.0 RESPONSIBILITIES:

Primary information security roles:

- 6.1 **Technology governance** endorses information security strategies and countywide information security policies, standards and guidelines.
- 6.2 **Chief Information Officer** oversees development and adoption of countywide information security policies and standards, and the strategic direction for managing King County's information security.
- 6.3 **TMB security sub team** develops countywide information security policies, standards and guidelines, plans and executes security initiatives, and reports on the county's information security health to the chief information officer.

- 6.4 **Organization** is accountable for the organization's information security practices to protect the operations and assets under their control, manages the organization's information security, ensures organization compliance with information security policies and standards, implements, manages and supports information systems in compliance with information security policies, standards and procedures, and securely uses information and information systems.

7.0 POLICY GUIDELINES:

None.